

PROBLEMS, SHEET 4, MP313, Semester 2, 1999.

1. Let  $m, k \in \mathbb{N}$ ,  $m > 1$  and let  $i + 1$  be the number of binary digits of  $k$ . Let  $x_0 = 2^{1+\lfloor i/m \rfloor}$ . Prove

$$k^{1/m} < x_0 < 2k^{1/m}.$$

2. Evaluate the Legendre symbols  $\left(\frac{2}{137}\right)$ ,  $\left(\frac{3}{137}\right)$ ,  $\left(\frac{53}{137}\right)$ ,  $\left(\frac{111}{1151}\right)$ .
3. (i) Prove that  $\left(\frac{-2}{p}\right) = 1 \Leftrightarrow p \equiv 1 \text{ or } 3 \pmod{8}$ ;  
(ii) Prove that  $\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv 1 \text{ or } 4 \pmod{5}$ .
4. Apply Serret's algorithm to express primes 137 and  $10^{50} + 577$  as sums of two squares.
5. If  $p$  is a prime and  $p = x^2 + ny^2$ , where  $x, y, n \in \mathbb{Z}$ , prove that  $\gcd(x, y) = 1$  and  $\left(\frac{-n}{p}\right) = 1$ .
6. (Wilson's theorem) Let  $p$  be a prime. By grouping integers  $x, y$  in the range  $1 \leq x < y \leq p - 1$  as products  $xy$ , where  $xy \equiv 1 \pmod{p}$ , prove that  $(p - 1)! \equiv -1 \pmod{p}$ .
7. Let  $p$  be an odd prime not dividing  $b$ . Define a 1-1 mapping  $y = f(x)$  of  $\{x \in \mathbb{N} \mid 1 \leq x \leq p - 1\}$  onto itself, by  $xy \equiv b \pmod{p}$ .

- (i) If  $\left(\frac{b}{p}\right) = -1$ , show that the mapping has no fixed points and deduce that

$$(p - 1)! \equiv b^{\frac{p-1}{2}} \pmod{p}.$$

- (ii) If  $\left(\frac{b}{p}\right) = 1$ , show that the mapping has two fixed points and deduce that

$$(p - 1)! \equiv -b^{\frac{p-1}{2}} \pmod{p}.$$

(In view of Wilson's theorem, this gives another proof of Euler's criterion.)

8. If  $p$  is an odd prime, not dividing  $k$ , show that

$$\sum_{x=1}^{p-1} \left( \frac{x(x+k)}{p} \right) = -1.$$

(Hint: Define  $y$  by  $xy \equiv 1 \pmod{p}$ ,  $1 \leq y \leq p-1$  and write the sum as

$$\sum_{x=1}^{p-1} \left( \frac{xy(xy+ky)}{p} \right).$$

9. Show that 65 is a strong pseudoprime to the base 8 but not to the base 14.